#4

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL

Docket Number:			
10746/31			
Application Number	Filing Date	Examiner	Art Unit
10/080,647	**February 22, 2002**	**Not Yet Assigned**	**2131**

Invention Title
DISTRIBUTED DIGITAL SIGNATURE GENERATION METHOD AND DIGITALLY SIGNED DIGITAL DOCUMENT GENERATION METHOD AND APPARATUS

Inventor(s)
HORITA et al.

Assistant Commissioner
for Patents
Washington, DC 20231

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on
Date: 4/22/2002 Reg. No. 33,865
Signature: Aaron C. Deditch

CLAIM TO CONVENTION PRIORITY UNDER 35 U.S.C. 119

SIR:

Claim to Convention Priority Date of Japanese Patent Application No. 2001-047338, filed in Japan on February 22, 2001, was made at the time this United States application was filed. In order to complete the claim to Convention Priority Date under 35 U.S.C. 119, a certified copy of this Japanese Application is enclosed herewith.

Dated: 4/22/2002

Aaron C. Deditch (Reg. No. 33,865)

KENYON & KENYON
One Broadway
New York, N.Y. 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)
CUSTOMER NO. 26646

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this office.

Date of Application: February 22, 2001

Application Number: No. 2001-047338
[ST.10/C]: [JP 2001-047338]

Applicant(s) NIPPON TELEGRAPH AND TELEPHONE CORPORATION

March 15, 2002

Commissioner,
Patent Office Kouzo Oikawa (Seal)

Certificate No.2002-3016959

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　２月２２日

出願番号
Application Number: 特願２００１－０４７３３８

[ST.10/C]: [ＪＰ２００１－０４７３３８]

出願人
Applicant(s): 日本電信電話株式会社

２００２年　３月１５日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願
【整理番号】　NTTH126715
【提出日】　平成13年 2月22日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　G09C　1/00
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　堀田　英一
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小野　諭
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体

【特許請求の範囲】

【請求項１】　ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名作成方法において、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分ディジタル署名を作成し、

各々のディジタル署名装置において、作成された前記部分ディジタル署名或いは入力された前記ディジタル文書と該部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成することを特徴とする分散ディジタル署名作成方法。

【請求項２】　入力された前記ディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、前記統合ディジタル署名を作成するために施す各部分ディジタル署名の前記変換処理の処理量を最小化する請求項１記載の分散ディジタル署名作成方法。

【請求項３】　前記部分ディジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する請求項１記載の分散ディジタル署名作成方法。

【請求項４】　ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名作成方法において、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

前記付加情報付ディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、

前記付加情報付ディジタル文書と前記部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された前記付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成することを特徴とする分散ディジタル署名作成方法。

【請求項５】　入力された前記ディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、前記統合ディジタル署名を作成するために施す各部分ディジタル署名の前記変換処理の処理量を最小化する請求項４記載の分散ディジタル署名作成方法。

【請求項６】　前記部分ディジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する請求項４記載の分散ディジタル署名作成方法。

【請求項７】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された該部分ディジタル署名或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段と、

出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段とを有す

ることを特徴とする分散ディジタル署名作成装置。

【請求項８】　前記統合ディジタル署名作成手段は、

入力された前記ディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、前記統合ディジタル署名を作成するために施す各部分ディジタル署名の前記変換処理の処理量を最小化する手段を含む請求項７記載の分散ディジタル署名作成装置。

【請求項９】　前記統合ディジタル署名作成手段は、

前記部分ディジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する手段を含む請求項７記載の分散ディジタル署名作成装置。

【請求項１０】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置であって、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と前記部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段と、

出力された前記付加情報付ディジタル文書と、前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段とを有することを特徴とする分散ディジタル署名作成装置。

【請求項１１】　前記統合ディジタル署名作成手段は、

入力された前記ディジタル文書に対して複数ある部分署名機関が作成した部分

ディジタル署名を閾値個数集めることにより、前記統合ディジタル署名を作成するために施す各部分ディジタル署名の前記変換処理の処理量を最小化する手段を含む請求項１０記載の分散ディジタル署名作成装置。

【請求項１２】　前記統合ディジタル署名作成手段は、

前記部分ディジタル署名を前記閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する手段を含む請求項１０記載の分散ディジタル署名作成装置。

【請求項１３】　ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成方法において、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分ディジタル署名を作成し、

各々のディジタル署名装置において、作成された前記部分ディジタル署名或いは入力された前記ディジタル文書と該部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成し、

入力されたディジタル文書と、作成された前記統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成することを特徴とするディジタル署名付ディジタル文書作成方法。

【請求項１４】ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成方法において、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

前記付加情報付ディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、

前記付加情報付ディジタル文書と前記部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された前記付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成し、

生成された前記付加情報付ディジタル文書と作成された前記統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成することを特徴とするディジタル署名付ディジタル文書作成方法。

【請求項１５】　ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成装置であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された前記部分ディジタル署名或いは入力された前記ディジタル文書と該部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段と、

各ディジタル署名装置から出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段と、

入力されたディジタル文書と、作成された前記統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成する文書作成手段とを有することを特徴とするディジタル署名付ディジタル文書作成装置。

【請求項１６】ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成装置であって、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合手

段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付ディジタル文書のハッシュ値に対して前記部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と前記部分ディジタル署名の組を出力する部分ディジタル署名作成手段と、

各ディジタル署名装置から出力された前記付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段と、

生成された前記付加情報付ディジタル文書と作成された前記統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成する文書作成手段とを有することを特徴とするディジタル署名付ディジタル文書作成装置。

【請求項１７】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムであって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された該部分ディジタル署名或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する部分ディジタル署名作成プロセスと、

出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有することを特徴とする分散ディジタル署名作成プログラム。

【請求項１８】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プロ

グラムであって、

入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と前記部分ディジタル署名の組を出力する複数の部分ディジタル署名作成プロセスと、

出力された前記付加情報付ディジタル文書と、前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有することを特徴とする分散ディジタル署名作成プログラム。

【請求項１９】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムを格納した記憶媒体であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された該部分ディジタル署名或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する部分ディジタル署名作成プロセスと、

出力された前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有することを特徴とする分散ディジタル署名作成プログラムを格納した記憶媒体。

【請求項２０】　ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プロ

グラムを格納した記憶媒体であって、

入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、前記付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と前記部分ディジタル署名の組を出力する複数の部分ディジタル署名作成プロセスと、

出力された前記付加情報付ディジタル文書と、前記部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有することを特徴とする分散ディジタル署名作成プログラムを格納した記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体に係り、特に、ディジタル文書に対するディジタル署名を作成するサービスにおいて、あるディジタル文書に対して、そのディジタル署名が存在するとき、当該ディジタル署名が偽造されたものではないこと、即ち、当該ディジタル署名が他の手段で作成されたものではないことを保証するための署名作成において、公開鍵暗号方式を用いた分散署名を複数の部分ディジタル署名機関が独立して行ない、分散署名機関で作成された部分ディジタル署名から一つの統合ディジタル署名を得るための分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体に関する。

【０００２】

詳しくは、複数ある分散署名機関のうち、一定数までのものが部分ディジタル署名作成時に不正な処理を行っても、その部分ディジタル署名から正しい統合ディジタル署名を得るための分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体に関する。

【０００３】

また、集中型のディジタル署名における秘密鍵の盗難などの危険性を排除するための分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体に関する。

【０００４】

また、一つの統合ディジタル署名を得るために複数ある分散部分ディジタル署名機関のうち、すべてのものが正しい部分ディジタル署名を作成しなければならないような従来型の分散型署名装置の耐攻撃性及び耐故障性における弱点を排除するための分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体に関する。

【０００５】

【従来の技術】

従来の公開鍵暗号方式に基づく分散ディジタル署名作成システムの多くは、分散された各々の部分ディジタル署名作成システムが部分ディジタル署名に用いる署名鍵を生成する際に、信頼される第三者機関を用いる。この場合、この第三者機関から署名鍵についての情報が漏洩する可能性があり、システムの中の一か所が秘密を漏洩するとシステムの安全性が全面的に損なわれるという弱点、即ち、秘密漏洩の単一点が存在するという弱点がある。

【０００６】

また、複数ある分散署名機関の全てのものが正しい部分ディジタル署名を作成しなければ部分ディジタル署名からディジタル署名を作成できないような分散ディジタル署名作成システムにおいては、複数ある分散署名機関の中で１つでも不

正な動作をするとディジタル署名が作成できないという耐攻撃性及び、耐故障性における弱点を有している。

【０００７】

上記のような、秘密漏洩上の弱点および耐郡家紀勢及び耐故障性における弱点を克服する分散ディジタル署名作成システムとしては、『T.Wu et al.: 「Building intrusion tolerant applications」,in Proceedings of 8th UNENIX Security Symposium, USENIX, 1999』（以下、第１の従来の方法）に報告されているものがある。当該システムは、部分ディジタル署名に用いる署名鍵を第三者機関を用いることなく、分散された複数の部分ディジタル署名作成機関の全体が分散処理により、各々の部分ディジタル署名作成機関を用いる部分署名鍵を作成し、さらに、それらの部分署名鍵についての部分的な情報を互いに交換することにより、複数ある部分ディジタル署名作成機関のうちの閾値と呼ばれる一定数のものが正常に動作すれば分散ディジタル署名作成を実行することができるシステムとなっている。

【０００８】

また、鍵情報が増大することを防ぐ方法として、『S.Miyazaki, K.Sakurai, M.Yung 「On threshold RSA-signing with no dealer 」in Proceedings of ICISC'99, pp.197-207, Sprinter, 1999』により提案されている。

また、信頼される第三者機関を用いるものではあるが、閾値個数の部分ディジタル署名を組み合わせて統合ディジタル署名を作成する方法で、かつ鍵情報が増大するという問題を解決する方法が、「V.Shoup 「Practical threshold signatures」, in Proceedings of Eurocrypto 2000.」（以下、第３の従来の方法）に提案されている。

【０００９】

また、特願平８－３５１５６５「階層を有する鍵管理方式及び暗号システム、分散ディジタル署名システム」（以下、第４の従来の方法）では、階層構造を持つような秘密鍵の閾値分散を用いた分散ディジタル署名システムが提案されている。この方式における秘密鍵の閾値分散の方法は、「R.L. Rivest, A. Shamir, and L. Adleman「A method for obtaining digital signature and public key

cryptosystems」Communications of ACM, Vol.21, pp.294-299, 1978」によるものであり、ディジタル署名を分散処理により作成するために、多項式補完式により元の秘密鍵を一度計算する方法をとっている。

【００１０】

また、公開鍵暗号方式に基づく分散処理機関を用いてディジタル文書に時刻印を押すサービスとして、特願平１１－２４７９９４号「分散型時刻認証装置及び方法と分散時刻認証プログラムを記録した記録媒体」（以下、第５の従来の方法）がある。当該文献で提案されている方式で実現する機能は、入力されたディジタル文書に付加する付加情報として時刻を用いることにより実現することができる。この分散型時刻認証装置は、一つの総合時刻署名を得るために複数ある分散時刻署名機関のうち全てのものが正しい部分時刻署名を作成しなければならないという特徴と、複数ある分散時刻署名機関のうちの一部が不正であれば、正しい時刻証明書が発行できないという特徴を有しており、一部の分散時刻署名機関による時刻証明書の偽造を防止する手段を提供している。

【００１１】

【発明が解決しようとする課題】

しかしながら、上記第１の従来の方法では、複数ある部分ディジタル署名作成システムのうちの閾値個数のどのグループが署名を作成するかに応じて、各部分ディジタル署名作成機関が用いる異なる部分署名鍵を用意する必要があり、そのため鍵情報が増大するという問題がある。

【００１２】

当該システムにおけるもう一つの問題点は、閾値個数のあるグループでディジタル署名を作成しようとして、その中の一部が正常に機能しないため署名作成に失敗した場合には、他の閾値個数のグループで署名を実行する必要があり、複数ある部分ディジタル署名作成機関における部分ディジタル署名の作成の処理量、及び統合ディジタル署名作成機関と複数ある部分ディジタル署名作成機関の間の通信が増大するということである。

【００１３】

また、上記第２の従来の方法は、第１の従来の方法の２つの問題点のうち鍵情

報が増大するという問題点を克服することは可能であるが、しかし、この方法においても部分ディジタル署名機関の閾値個数のあるグループが署名作成に失敗した場合に、部分ディジタル署名作成の処理量及び統合ディジタル署名作成機関と複数ある部分ディジタル署名作成機関の間の通信量が増大するという第２の問題点は残されている。また、部分ディジタル署名からディジタル署名を作成する処理量が部分ディジタル署名作成機関の数が増えるに従って増大し、署名作成処理全体の処理量が大きくなるということも問題である。また、部分ディジタル署名の正当性を検証するための処理量が大きく、そのため作成された統合ディジタル署名が正しい部分署名鍵から作成された部分ディジタル署名のみを組み合わせて作られたものであることを保証するための処理量が大きいことも問題である。

【００１４】

また、上記第３の従来の方法は、閾値個数の部分ディジタル署名を組み合わせて統合ディジタル署名を作成する方法で、かつ鍵情報が増大するという問題を解決することはできるが、当該方法においても部分ディジタル署名からディジタル署名を作成する処理量が部分ディジタル署名機関の数が増えるに従って増大し、署名作成処理全体の処理量が大きくなるという問題がある。また、部分ディジタル署名が正しい部分署名鍵から作成された部分ディジタル署名のみを組み合わせて作られたものであることを保証するための処理量が大きいことも問題である。

また、上記第４の従来の方法は、ディジタル署名を分散処理により作成するために、多項式補完式により元の秘密鍵を一度計算する方法をとっているため、この計算を実行する機関は秘密鍵の情報を知ることができ、秘密漏洩の単一点が存在するという弱点を伴うものとなっている。また、この文献においては、複数ある秘密価値の部分情報の保持機関が所定の数集まってディジタル署名の生成を試みる際に、それらの部分情報保持者の一部が不正な処理を行う場合に、どの部分情報保機関が不正を働いたかを識別し、その不正な機関を除いて正しい機関のみで効率的にディジタル署名を生成する方法については、述べられていない。

【００１５】

また、上記第５の従来の方法における分散型時刻認証装置は、複数のある分散時刻署名機関の中で１つでも不正な動作をすると時刻証明書が作成できないとい

う点が耐攻撃性及び耐故障性における弱点となっている。

【００１６】

本発明は、上記の点に鑑みなされたもので、従来の信頼される第三者機関を用いた分散ディジタル署名作成システムが持つ、秘密漏洩の単一点が存在するという問題点を解決し、かつ複数ある部分ディジタル署名機関のすべてのものが正しい部分ディジタル署名を作成しなければ部分ディジタル署名からディジタル署名を作成できないような分散ディジタル署名作成システムを持つ、複数ある分散署名機関の中で１つでも不正な動作をするとディジタル署名が作成できないという耐攻撃性及び耐故障性における弱点を解決した分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体を提供することを目的とする。

【００１７】

また、本発明の目的は、入力されたディジタル文書に対して、複数ある部分ディジタル署名機関が作成した部分ディジタル署名を閾値個数集めることにより、当該ディジタル文書に対するディジタル署名を作成する閾値分散署名システムにおける、複数ある部分ディジタル署名機関の閾値個数のあるグループが署名の作成に失敗した場合に、部分ディジタル署名作成の処理量及び統合ディジタル署名作成機関と複数ある部分ディジタル署名作成機関の間の通信が増大するという問題点を解決した分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体を提供することである。

【００１８】

更なる本発明の目的は、部分ディジタル署名からディジタル署名を作成するための処理量が大きいという問題を解決した分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体を提供することである。

【００１９】

また、更なる目的は、作成されたディジタル署名が正しい部分署名鍵から作成された部分ディジタル署名のみを組み合わせて作られたという意味で正しいものであることを保証するための処理量が大きいという問題点を解決した分散ディジタル署名作成方法及び装置及び分散ディジタル署名付ディジタル文書作成方法及び装置及び分散ディジタル署名作成プログラム及び分散ディジタル署名作成プログラムを格納した記憶媒体を提供することである。

【００２０】

【課題を解決するための手段】

図１は、本発明の原理を説明するための図である。

【００２１】

本発明（請求項１）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名作成方法において、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し（ステップ１）、

入力されるディジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分ディジタル署名を作成し（ステップ２）、

各々のディジタル署名装置において、作成された部分ディジタル署名或いは入力されたディジタル文書と該部分ディジタル署名の組を出力し（ステップ３）、

各ディジタル署名装置から出力された部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する（ステップ４）。

【００２２】

本発明（請求項２）は、入力されたディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、統合ディジタル署名を作成するために施す各部分ディジタル署名の変換処理の処理量を最小化する。

【００２３】

本発明（請求項３）は、部分ディジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する。

【００２４】

本発明（請求項４）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名作成方法において、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

付加情報付ディジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、

付加情報付ディジタル文書と部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する。

【００２５】

本発明（請求項５）は、入力されたディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、統合ディジタル署名を作成するために施す各部分ディジタル署名の変換処理の処理量を最小化する。

【００２６】

本発明（請求項６）は、部分ディジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する。

【００２７】

図２は、本発明の原理構成図である。

【００２８】

本発明（請求項７）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置１であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書Ｍのハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名１６を作成し、作成された該部分ディジタル署名１６或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段１３と、

出力された部分ディジタル署名１６を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段１４とを有する。

【００２９】

本発明（請求項８）は、統合ディジタル署名作成手段１４において、

入力されたディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、統合ディジタル署名を作成するために施す各部分ディジタル署名の変換処理の処理量を最小化する手段を含む。

【００３０】

本発明（請求項９）は、統合ディジタル署名作成手段１４において、

部分ディジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する手段を含む。

【００３１】

本発明（請求項１０）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置であって、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段と、

出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段とを有する。

【００３２】

本発明（請求項１１）は、統合ディジタル署名作成手段において、

入力されたディジタル文書に対して複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、統合ディジタル署名を作成するために施す各部分ディジタル署名の変換処理の処理量を最小化する手段を含む。

【００３３】

本発明（請求項１２）は、統合ディジタル署名作成手段において、

部分ディジタル署名を閾値の数だけ組み合わせ、署名検証処理を行うことにより、不正な部分署名鍵を用いて作成された不正な部分ディジタル署名の存在を判定し、かつ不正な部分ディジタル署名を特定する手段を含む。

【００３４】

本発明（請求項１３）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成方法において、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、

入力されるディジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分ディジタル署名を作成し、

各々のディジタル署名装置において、作成された部分ディジタル署名或いは入

力されたディジタル文書と該部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成し、

入力されたディジタル文書と、作成された統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成する。

【００３５】

本発明（請求項１４）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成方法において、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力し、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、

付加情報付ディジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、

付加情報付ディジタル文書と部分ディジタル署名の組を出力し、

各ディジタル署名装置から出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成し、

生成された付加情報付ディジタル文書と作成された統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成する。

【００３６】

本発明（請求項１５）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成装置であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のた

めに用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された部分ディジタル署名或いは入力されたディジタル文書と該部分ディジタル署名の組を出力する複数の部分ディジタル署名作成手段と、

各ディジタル署名装置から出力された部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段と、

入力されたディジタル文書と、作成された統合ディジタル署名とを含むディジタル署名付ディジタル文書を作成する文書作成手段とを有する。

【００３７】

本発明（請求項１６）は、ディジタル文書に対するディジタル署名を複数の署名装置で分散して作成する分散ディジタル署名付ディジタル文書作成装置であって、

各々の署名装置に対して、入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合手段と、

信頼される第三者機関を用いることなく、各々の署名装置において部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付ディジタル文書のハッシュ値に対して部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と部分ディジタル署名の組を出力する部分ディジタル署名作成手段と、

各ディジタル署名装置から出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成手段と、

生成された付加情報付ディジタル文書と作成された統合ディジタル署名とを含

むディジタル署名付ディジタル文書を作成する文書作成手段とを有する。

【００３８】

本発明（請求項１７）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムであって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された該部分ディジタル署名或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する部分ディジタル署名作成プロセスと、

出力された部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有する。

【００３９】

本発明（請求項１８）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムであって、

入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と部分ディジタル署名の組を出力する複数の部分ディジタル署名作成プロセスと、

出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジ

タル署名作成プロセスとを有する。

【００４０】

本発明（請求項１９）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムを格納した記憶媒体であって、

信頼される第三者機関を用いることなく、各々が部分ディジタル署名作成のために用いる部分署名鍵を互いに通信しながら分散処理により作成し、入力されるディジタル文書のハッシュ値に対して該部分署名鍵を用いて、各々の部分ディジタル署名を作成し、作成された該部分ディジタル署名或いは入力された該ディジタル文書と該部分ディジタル署名の組を出力する部分ディジタル署名作成プロセスと、

出力された部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有する。

本発明（請求項２０）は、ディジタル文書に対するディジタル署名を分散処理により作成する分散ディジタル署名作成装置に実行させる分散ディジタル署名作成プログラムを格納した記憶媒体であって、

入力されるディジタル文書に、各々１個以上の付加情報を付加して１個以上の付加情報付ディジタル文書を出力する付加情報結合プロセスと、

信頼される第三者機関を用いることなく、部分ディジタル署名作成のために用いる部分署名鍵を署名装置間で互いに通信しながら分散処理により作成し、付加情報付ディジタル文書のハッシュ値に対して該部分署名鍵を用いて、部分署名鍵を各々の部分ディジタル署名を作成し、該付加情報付ディジタル文書と部分ディジタル署名の組を出力する複数の部分ディジタル署名作成プロセスと、　出力された付加情報付ディジタル文書と、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせ、該組み合わせに応じた変換処理を各部分ディジタル署名に施し、該変換処理の結果から統合ディジタル署名を作成する統合ディジタル署名作成プロセスとを有する。

【００４１】

上記のように、本発明（請求項１、７、１７、１９）によれば、入力されるディジタル文書に対して、部分ディジタル署名の閾値個数のある集合を用いて統合ディジタル署名が作れない場合にも、新たに部分ディジタル署名の作成を部分ディジタル署名作成手段に依頼することなく、最初に集まった部分ディジタル署名の全集合の中から他の閾値個数の集合を選び、統合ディジタル署名の作成を行う。これにより、閾値個数のある部分ディジタル署名作成手段の集合でディジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分ディジタル署名作成手段における部分ディジタル署名の作成の処理量、及び統合ディジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するという問題点を解決することが可能となる。

【００４２】

また、本発明（請求項４、１０、１８、２０）によれば、入力されるディジタル文に付加情報を加えたものに対して部分ディジタル署名の閾値個数のある集合を用いて統合ディジタル署名が作れない場合にも、新たに部分ディジタル署名の作成を部分ディジタル署名作成手段に依頼することなく、最初に集まった部分ディジタル署名の全集合の中から他の閾値個数の集合を選び、統合ディジタル署名の作成を行う。これにより、閾値個数のある部分ディジタル署名作成手段の集合でディジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分ディジタル署名の作成の処理量及び、統合ディジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するいう問題を解決することが可能となる。

【００４３】

また、本発明（請求項２、５、８、１１）では、入力されたディジタル文書に対して、複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、当該ディジタル文書に対するディジタル署名を作成する閾値分散署名システムにおける、部分ディジタル署名からディジタル署名を作成するための処理量が大きいという問題点を解決することが可能となる。

【００４４】

また、本発明（請求項３、９）では、入力されたディジタル文書に対して、複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、該ディジタル文書に対するディジタル署名を作成する閾値分散署名システムにおける、作成されたディジタル署名が正しい部分署名鍵から作成された部分ディジタル署名のみを組み合わせて作られたという意味で正しいものであることを保証するための処理量が大きいという問題点を解決することが可能となる。

【００４５】

また、本発明（請求項６、１２）は、入力されたディジタル文書に対して、複数ある部分署名機関が作成した部分ディジタル署名を閾値個数集めることにより、当該ディジタル文書に対するディジタル署名を作成する閾値分散署名システムにおける作成されたディジタル署名が正しい部分署名鍵から作成された部分ディジタル署名のみを組み合わせて作られたという意味で正しいものであることを保証するための処理量が大きいという問題点を解決することが可能となる。

【００４６】

また、本発明（請求項１３、１５）は、入力されるディジタル文書に対して、ディジタル署名付ディジタル文書を作成する処理の中で、部分ディジタル署名の閾値個数のある集合を用いて統合ディジタル署名が作れない場合にも、新たに部分ディジタル署名の作成を部分ディジタル署名作成手段に依頼することなく、最初に集まった部分ディジタル署名の全集合の中から他の閾値個数の集合を選び、統合ディジタル署名の作成を行ない、それと入力されたディジタル文書を組み合わせて、ディジタル署名付ディジタル文書を作成する。これにより、閾値個数のある部分ディジタル署名作成手段の集合でディジタル署名を作成しようとして、その中の一部が正常に機能しないため署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分ディジタル署名の作成の処理量、及び統合ディジタル署名作成機関と複数ある部分署名作成機関の通信が増大するという問題を解決することが可能となる。

【００４７】

また、本発明（請求項１４、１６）は、入力されるディジタル文書に対して、付加情報付ディジタル文書を作成し、当該付加情報付ディジタル文書に対するデ

ィジタル署名付ディジタル文書を作成する処理の中で、部分ディジタル署名の閾値個数のある集合を用いて、統合ディジタル署名が作れない場合にも、新たに部分ディジタル署名の作成を部分ディジタル署名作成手段に依頼することなく、最初に集まった部分ディジタル署名の全集合の中から他の閾値個数の集合を選び、統合ディジタル署名の作成を行ない、それと入力されたディジタル文書を組み合わせて、ディジタル署名付ディジタル文書を作成する。これにより、閾値個数のある部分ディジタル署名作成手段の集合でディジタル署名を作成しようとして、その中に一部が正常に機能しないための署名の作成に失敗した場合に、複数ある部分署名作成システムにおける部分ディジタル署名の作成の処理量、及び統合ディジタル署名作成機関と複数ある部分署名作成機関の間の通信が増大するという問題を解決することが可能となる。

【００４８】

【発明の実施の形態】

本発明は、以下の図３から図５に示す３つの閾値分散ディジタル署名作成装置を提案している。

【００４９】

図３は、本発明の閾値分散ディジタル署名作成装置の構成図（その１）である。

【００５０】

同図において、分散ディジタル署名作成装置１は、複数の部分ディジタル署名作成部１３と、統合ディジタル署名作成部１４とを有する。

【００５１】

部分ディジタル署名作成部１３は、入力されたディジタル文書Mに対して各々独立に部分ディジタル署名

$$S1\ (M),\ \cdots,\ Sr\ (M)$$

を作成する。

【００５２】

統合ディジタル署名作成部１４は、数の部分ディジタル署名作成部１３１、…，１３ｒと、当該複数の部分ディジタッル署名作成部１３で独立に作成されたｍ

個の部分ディジタル署名

$$Sr(1)(M), \cdots, Sr(m)(M),$$

（k≦m≦rかつ1≦r（1），…，r（m）≦r）及び当該ディジタル文書Mを受け取り、予め定めた閾値の個数k個の部分ディジタル署名作成部１３の識別番号からなる1以上であるs個の集合

$$I1, \cdots, Is$$

に対して、出力された部分ディジタル署名から複数の統合ディジタル署名

$$S(M, I1), \cdots, S(M, Is)$$

を作成する。

【００５３】

図４は、本発明の閾値分散ディジタル署名作成装置の構成図（その２）である。

【００５４】

同図に示すディジタル署名作成装置１は、図３の構成と同様であるが、部分ディジタル署名作成部１３は、入力されたディジタル文書Mに対して各々独立にディジタル文書と部分ディジタル署名の組

$$(M, S1(M)), \cdots, (M, Sr(M))$$

を作成する。

【００５５】

また、同図における統合ディジタル署名作成部１４は、当該ディジタル文書Mと、当該複数の部分ディジタル署名作成部１３で独立に作成された部分ディジタル署名のm個の組

$$(M, Sr(1)(M)), \cdots, (M, Sr(m)(M)$$

（k≦m≦rかつ1≦r（1），…，r（m）≦r）を受け取り、予め定められている閾値の個数k個の部分ディジタル署名作成部１３の識別番号からなる1以上であるs個の集合

$$I1, \cdots, Is$$

に対して、出力された部分ディジタル署名から複数の統合ディジタル署名

$$S(M, I1), \cdots, S(M, Is)$$

を作成する。

【００５６】

図５は、本発明の閾値分散ディジタル署名作成装置の構成図（その３）である。同図において、分散ディジタル署名作成装置１は、複数の付加情報結合部１２、複数の部分ディジタル署名作成部１３、及び統合ディジタル署名作成部１４から構成される。

【００５７】

付加情報結合部１２は、入力されたディジタル文書Mに対して各々独立に１以上ν（ｉ）個の付加情報

$$\alpha(i, 1), \cdots, \alpha(i, \nu(i))$$

を作成して、文書Mと、

$$\alpha(i, 1), \cdots, \alpha(i, \nu(i))$$

を結合してできる付加情報付ディジタル文書

$$M \| \alpha(i, 1), \cdots, M \| \alpha(i, \nu(i))$$

を作成する。

【００５８】

複数のディジタル署名作成部１３ｉ（$1 \leqq i \leqq r$）は、付加情報結合部１２１，…，１２ｒに対して、各々に対応して存在し、付加情報結合部１２によって生成された付加情報付ディジタル文書

$$M \| \alpha(i, 1), \cdots, M \| \alpha(i, \nu(i))$$

に対して、各々独立に付加情報ディジタル文書とその部分ディジタル署名の組、

$(M \| \alpha(i, 1), Si\ (M \| \alpha(i, 1))), \cdots,$

$(M \| \alpha(i, \nu(i)), Si\ (M \| \alpha(i, \nu(i))))$

を作成する。

【００５９】

統合ディジタル署名作成部１４は、当該複数の部分ディジタル署名作成部１３で独立に作成された付加情報付ディジタル文書

$$M \| \alpha(i, h(i))$$

とその部分ディジタル署名のｍ個の組

（M’，Sr(1)（M’）），…，（M’，Sr(m)，（M’））

でｋ≦ｍ≦ｒかつ１≦ｒ（１），…，ｒ（ｍ）≦ｒかつ

M’∈｛M‖α（ｒ（ｉ），１），…，M‖α（ｒ（ｉ），ν（ｉ））｝

（１≦ｉ≦ｍ）となるようなものを選び、さらに、予め定めた閾値の個数ｋ個の部分ディジタル署名作成部１３の識別番号からなる１以上であるｓ個の集合

Ｉ１，…，Ｉｓ⊆｛ｒ（１），…，ｒ（ｍ）｝

を選び、それらに対して１以上であるｓ個の統合ディジタル署名

Ｓ（Ｍ’，Ｉ１），…，Ｓ（Ｍ’，Ｉｓ）

を作成する。

【００６０】

付加情報結合部１２が結合する付加情報としては、ディジタル署名作成機関の識別情報、ディジタル署名の有効期限、ディジタル署名作成の時刻、及びそれらの組み合わせ等が考えられる。

【００６１】

【実施例】

以下、図面と共に本発明の実施例を説明する。

【００６２】

以下、前述の図３、図４、図５を用いて、ディジタル署名作成について、１例をあげて説明する。なお、ここでは、公開鍵暗号の具体例として、ＲＳＡを用いる。ＲＳＡについては、R.L. Rivest, A. Shamir, and L. Adleman「A method for obtaining digital signature and public key cryptosystems」Communications of ACM, Vol.21,pp.294-299,1978 に詳述されている。

最初に、部分署名作成のための部分ディジタル署名作成部間の準備手順について説明する。

まず、Ｎを十分大きな２つの素数の積とし、φ（Ｎ）を０≦ｉ＜ＮでＮと互いに素な整数ｉの個数とする。次に、ｅを部分ディジタル署名作成部１３の個数ｒより小さい因数をもたなくかつφ（Ｎ）と互いに素な整数とする。

【００６３】

ＮとｅのＮ，ｅ）を公開鍵とする。

【００６４】

$$e \cdot (d1 + \cdots dr) \equiv 1 \mod \phi(N)$$

となる整数の組ｄ１，…，ｄｒを、D.Boneh et al.: Efficient generation of shared RSA key(extended abstract), in "Proceedings Crypto'97(Sprinter,97)で提案されている方法等を用いて分散生成し、各ｉ＝１，…，ｒに対して部分ディジタル署名作成部１３がｄｉを保持するようにする。

【００６５】

ここで、

$$d = (d1 + \cdots dr)$$

と置くと、これが公開鍵（Ｎ，ｅ）に対応する秘密鍵になる。但し、各々の部分ディジタル署名作成部１３ｉ、図３、図４、図５の部分ディジタル署名作成部１３ｉはｄｉを知るのみであり、どの部分ディッジタル署名作成部１３も知ることはなく、かつ統合ディジタル署名作成部１４もｄを知ることはない。

【００６６】

ｋを分散署名作成のために必要となる部分署名の最低限の数、即ち、閾値とし、各部分ディジタル署名作成部１３ｉはｋ個の十分大きな整数係数

$$ai,0 = di,\ ai,\ \cdots,\ ai,k-1$$

を選び、多項式ｆｉ（ｘ）を

$$fi(x) = ai,0 + ai,1 \cdot x + \cdots + ai,k-1 \cdot x^{k-1}$$

と置く（$1 \leqq i \leqq r$）。

【００６７】

各部分ディジタル署名作成部１３ｉは、$1 \leqq j \leqq r$かつ、$j \neq i$なる整数ｊに対して、

$$fi(j)$$

を計算し、部分ディジタル署名作成部１３ｊに送信し、また、ｆｉ（ｉ）を計算する。

【００６８】

各部分ディジタル署名作成部１３ｉは、他の各部分ディジタル署名作成部１３ｊから送られてきたｆｉ（ｉ）の値（$j \neq i$かつ$1 \leqq j \leqq r$）と、自分で計算し

たｆｉ（ｉ）の和を計算し、Ｄ（ｉ）と置く。即ち、

【００６９】

【数１】

$$D(i)=\sum_{1\leq j\leq r} f_j(i)$$

と置く。

【００７０】

Ｄ（ｉ）を、部分ディジタル署名作成部１３ｉの部分署名鍵と呼ぶ（１≦ｉ≦ｒ）。

【００７１】

次に、各部分ディジタル署名作成部１３における部分ディジタル署名作成の手順について説明する。

【００７２】

図３及び図４の構成では、各部分ディジタル署名作成部１３ｉは、値域が｛０，１，…，Ｎ－１｝に含まれるような適当なハッシュ関数Ｈ（例えば、ＳＨＡ－１，やＭＤ５）を用いて入力されたディジタル文書Ｍに対して

$$Si(M)=H(M)^{D(i)} \bmod N$$

を計算し、これをＭに対する部分ディジタル署名とする（１≦ｉ≦ｒ）。

【００７３】

図５の構成における各部分ディジタル署名作成部１３ｉは、値域が｛０，１，…，Ｎ－１｝に含まれるような適当なハッシュ関数（例えば、ＳＨＡ－１やＭＤ５）Ｈを用いて付加情報結合部１２から出力された付加情報付ディジタル文書Ｍ‖α（ｉ，ｊ）に対して、

$$Si(M\|\alpha(i,j))=H(M\|\alpha(i,j))^{D(i)} \bmod N$$

を計算し、これをＭ‖α（ｉ，ｊ）に対する部分ディジタル署名とする（ｉ≦ｉ≦ｒ）。

【００７４】

次に、統合ディジタル署名作成部１４における統合ディジタル署名作成の手順

について説明する。

【００７５】

図３、図４の部分ディジタル署名作成部１３ｉが作成する部分ディジタル署名Ｓｉ（Ｍ）に対して、Ｍを当該部分ディジタル署名の被署名ディジタル文書と呼ぶ。図５の部分ディジタル署名作成部１３ｉが作成する部分ディジタル署名

Ｓｉ（Ｍ‖α（ｉ，ｊ））

に対しては、付加情報付ディジタル文書Ｍ‖α（ｉ，ｊ）を当該部分ディジタル署名の被署名ディジタル文書と呼ぶ。

【００７６】

１≦ｒ（１），…，ｒ（ｋ）≦ｋ≦ｒでｒ（１），…ｒ（ｋ）は互いに異なり

Ｓｒ(1)（Ｍ’），…，Ｓｒ(k)（Ｍ’）

を閾値個数の部分ディジタル署名の集合で、各々被署名ディジタル文書がＭ’に一致するものとするとき、統合ディジタル署名作成部１４が部分ディジタル署名

Ｓｒ(1)（Ｍ’），…Ｓｒ(k)（Ｍ’）

を基に、統合ディジタル署名Ｓ（Ｍ’，Ｉ）を作成する手順は以下の通りである。Ｉ＝｛ｒ（１），…，ｒ（ｋ）｝とおき、さらに、各ｉ∈Ｉに対して

【００７７】

【数２】

$$\lambda(I, i) = \prod_{j \in I,\ j \neq i} \frac{j}{j - i}$$

と置く。

【００７８】

正整数Δ（Ｉ）をｅと互いに素で、かつ各ｉ∈ｉについて、

Δ（Ｉ）・λ（Ｉ，ｉ）

が整数となるように選ぶ。以下、Δ（Ｉ）をＩについての部分ディジタル署名の変換指数と呼ぶ。このような変換指数としては、例えば、『S.Miyazaki, K.Sakurai, M.Yung 「On threshold RSA-signing with no dealer」 in Proceedings o

f ICISC799, pp.197-207, Sprinter, 1999』に提案されているように、Ｉによらず、常に（（ｒ－１）！）^{2} を選ぶことができるが、以下に述べるように総合ディジタル署名作成の処理量が小さくなるような他の取り方も可能である。

【００７９】

各ｉ∈Ｉに対して、

$$\Lambda(I, i) = \Delta(I) \cdot \lambda(I, i)$$

を計算する。

【００８０】

部分ディジタル署名に対してＳr(i)（M'）のΛ（Ｉ，ｉ）乗をmod Ｎでとるという変換処理を施し、その結果をＴr(i)（M'）とおく。即ち、

【００８１】

【数３】

$$T_{r(i)}(M') = S_{r(i)}(M')^{\Lambda(I, i)} \bmod N$$

と置く。

【００８２】

Tr(1)（M'），…，Tr(k)（M'）を乗算し、

【００８３】

【数４】

$$w(I) = \left(\prod_{i \in I} T_{r(i)}(M') \right) \bmod N$$

を計算する。

【００８４】

Δ（Ｉ）は、ｅと互いに素であるので、拡張ユークリッド互除法を用いて、

$$\Delta(I) \cdot a(I) + e \cdot b(I) = 1$$

となるような整数ａ（Ｉ）とｂ（Ｉ）が計算可能である。これらを計算する。

【００８５】

上記のａ（Ｉ），ｂ（Ｉ），ｗ（Ｉ）を用いて、

$$S(M', I) = w(I)^{a(I)} \cdot H(M')^{b(j)} \bmod N$$

を計算し、これを被署名ディジタル文書Ｍ’に対する統合ディジタル署名とする。

【００８６】

図６は、本発明の一実施例の処理量が最小となるような部分ディジタル署名に対する変換指数の計算手順を示す図である。

【００８７】

上記の部分ディジタル署名から統合ディジタル署名を作成する処理において、各々の閾値個数の部分ディジタル署名作成部１３の識別番号の集合

$$I = \{r(1), \cdots, r(k)\}$$

に対して変換指数と呼ばれる正整数Δ（Ｉ）をｅと互いに素で、かつ各ｉ∈Ｉについて、

$$\Delta(I) \cdot \lambda(I, i)$$

が整数となるように選ぶことが必要である。このような変換指数の取り方としては、『S. Miyazaki et al.「On threshold RSA-signing with no dealer」in Proceedings of ICISC'99, LNCS Vol.1787, pp. 197-207, Sprinter, 1999』において、Ｉによらず、常にｒ－１の階乗の２乗、即ち、$((r-1)!)^2$をとることが提案されている。ここで、ｒは、部分署名作成機関の総数である。図６は、部分ディジタル署名作成部１３の識別番号の集合Ｉに応じて、部分ディジタル署名から統合ディジタル署名を作成するために必要な処理量が最小となるという意味で最適となるような変換指数をとる手順を示したものである。閾値個数の部分ディジタル署名作成部１３の識別番号の集合$i = \{r(1), \cdots, r(k)\}$が与えられたものとする。

【００８８】

第１のステップ４１において、各ｉ∈Ｉに対して、

【００８９】

【数５】

$$\lambda(I, i) = \prod_{j \in I,\ j \neq i} \frac{j}{j - i}$$

を計算する。

【００９０】

第２に、ステップ４２において、各ｉ∈Ｉに対して、λ（Ｉ，ｉ）を約分し、その結果の分母の絶対値をδ（Ｉ，ｉ）とおく。即ち、

【００９１】

【数６】

$$\lambda(I, i) = \frac{\gamma(I, i)}{\delta(I, i)}$$

で、δ（Ｉ，ｉ）＞０、γ（Ｉ，ｉ）とδ（Ｉ，ｉ）は互いに素な整数となるようにδ（Ｉ，ｉ）を決める。

【００９２】

第３に、ステップ４３において、δ（Ｉ，ｒ（１）），…，δ（Ｉ，ｒ（Ｋ））の最小公倍数を計算し、Δ（Ｉ）とおく。

【００９３】

以上により、Ｉについての部分ディジタル署名の変換指数Δ（Ｉ）が得られる。Δ（Ｉ）は、これを用いて部分ディジタル署名から統合ディジタル署名を作成するために必要な処理量が最小になるという意味で最適なものとなっている。例えば、『S.Miyazaki et al.「On threshold RSA-signing with no dealer」in Proceedings of ICISC'99, LNCS Vol.1787, pp. 197-207, Sprinter, 1999』で提案されているように部分ディジタル署名部の総数をｒとして

$$\Delta(I) = ((r-1)!)^2$$

とする場合に比較すると、署名に必要な閾値ｋが３から１０で部分署名作成部１３の数ｒが５から１９の場合、部分ディジタル署名から統合ディジタル署名を作成する処理量が約１／６倍に減少することが計算により確認できる。

【００９４】

次に、不正な部分ディジタル署名の存在の判定手順について説明する。

【００９５】

図７は、本発明の一実施例の部分ディジタル署名の組み合わせによる不正な部分ディジタル署名の検出法を説明するための図である。また、図８は、本発明の一実施例の部分ディジタル署名の組み合わせによる不正な部分ディジタル署名存在の判定手順のフローチャートであり、図９は、本発明の不正な部分ディジタル署名が１個のみか否かを判定し、１個のみ存在する不正な部分ディジタル署名を決定する手順のフローチャートである。

【００９６】

これらを用いて、図３、図４、図５で示された閾値分散ディジタル署名作成装置において、統合ディジタル署名作成部１４が部分署名を閾値の個数だけ組み合わせ署名検証処理を施すことにより、不正な部分署名鍵を用いて作成された不正な部分署名の存在を判定し、かつ不正な部分署名を特定する手順について説明する。

【００９７】

ｋを部分ディジタル署名から統合ディジタル署名を作成するために必要な閾値としたとき、図３、図４、図５の統合ディジタル署名作成部１４は、各々異なる部分署名作成部１３から出力されたもので、かつ被署名ディジタル文書が一致するようなｋ個の部分ディジタル署名、

$$Sr(1)(M'), \cdots, Sr(k)(M')$$

（ｒ（１），…，ｒ（ｋ）は互いに異なり、１≦ｒ（１），…，ｒ（ｋ）≦ｒ）から統合ディジタル署名

$$S(M', I)$$

を作成することができる。ここで、M’は、Ｓｒ(k)（M’）の被署名ディジタル文書とし、Ｉ＝｛ｒ（１），…，ｒ（ｋ）｝とおく。

【００９８】

このようなｋ個の部分ディジタル署名の種々の組み合わせに対して、統合ディジタル署名作成部１４は、作成されたＳ（M’，Ｉ）が被署名ディジタル文書M

’の署名になっているか否かを、公開鍵（ｅ，Ｎ）によるＳ（Ｍ’，Ｉ）の復号化が被署名ディジタル文書のハッシュ値Ｈ（Ｍ’）に一致するか否かを試験することにより判定する。このことにより、Ｓ（Ｍ’，Ｉ）が最初に与えられたディジタル文書の正しいディジタル署名となっているか否かを判定することができる。

【００９９】

先に述べたように、ディジタル署名Ｓ（Ｍ’，Ｉ）の被署名ディジタル文書Ｍ’は、付加情報が無い図３及び図４の構成のときは、Ｍであり、付加情報αがある図５の構成のときは、Ｍ‖αである。

【０１００】

被署名ディジタル文書Ｍ’は、図３の構成においては、最初から統合ディジタル署名作成部１３に入力されるものであり、図４、図５の構成においては、部分ディジタル署名Ｓｉ（Ｍ’）と対になって部分ディジタル署名作成部１３、図４及び図５の部分ディジタル署名作成部１３ｉ（１≦ｉ≦ｒ）から統合ディジタル署名作成部１４に出力されるものである。

【０１０１】

図８を用いて、図３、図４、図５の各々の部分ディジタル署名作成部１３ｉから送信されてきた、被署名ディジタル文書がＭ’に一致する、部分ディジタル署名の集合

$$Sr(1)(M'),\ \cdots,\ Sr(m)(M')$$

の中に、正しい部分署名が少なくとも総合署名作成のために必要な閾値ｋより１小さい数だけある場合に、

$$Sr(1)(M'),\ \cdots,\ Sr(m)(M')$$

の中に不正な部分署名が存在するか否かを判定する手順を示す。

【０１０２】

但し、ｋ＋１≦ｍ≦ｒで、ｒ（１），…，ｒ（ｍ）は互いに異なるものとする。ここで、ｍ＝ｒとしないのは、部分ディジタル署名作成部１３の一部が正常に動作せず、部分ディジタル署名を送信しない可能性があるからである。

【０１０３】

ステップ６１）　図７に示すように、ｍ個の個数ｋの｛ｒ（１），…，ｒ（ｍ））｝部分集合Ｉ（０），…，Ｉ（ｍ－１）を選ぶ。

【０１０４】

$$I(i)=\{r((j+1)\bmod m)+1 \mid 0\leqq j\leqq m-1\}$$

（但し、ｉ＝０，…，ｍ－１）

ステップ６２）　各Ｉ（ｉ）（ｉ＝０，…，ｍ－１）に対して

$$\{Sr(M') \mid r\in I(i)\}$$

から統合ディジタル署名Ｓ（Ｍ’，Ｉ（ｉ））を作成する。

【０１０５】

ステップ６３）　各Ｉ（ｉ）（ｉ＝０，…，ｍ－１）に対して、当該統合ディジタル署名の公開鍵（ｅ，Ｎ）による復号化

$$S(M', I(i))^{e} \bmod N$$

がＨ（Ｍ’）に一致するかどうかを試験する。

【０１０６】

ステップ６４）　全てのＩ（ｉ）（ｉ＝０，…，ｍ－１）に対して、上記ステップ６３で

$$S(M', I(i))^{e} \bmod N = H(M')$$

が成り立つことを確認できれば、

$$Sr(i)(M'), \cdots, Sr(m)(M')$$

の中に不正な部分署名が存在すると判定する。

【０１０７】

ｍ個の部分ディジタル署名

$$Sr(1)(M'), \cdots, Sr(m)(M')$$

のなかに不正な部分ディジタル署名が複数あり、それらが結託して互いの不正の効果を打ち消しあうことにより、０≦ｉ≦ｍ－１なる各Ｉ（ｉ）について、Ｓｒ（Ｍ’）（ｒ∈Ｉ（ｉ）から生成される統合ディジタル署名Ｓ（Ｍ’，Ｉ（ｉ））が正当な署名となるという可能性も想定されるが、３≦ｋ≦１０でｋ＋１≦ｒ≦２・ｋ－１という範囲ではこのようなことは起こらないことが計算機テストにより確認できる。

【０１０８】

次に、不正な部分ディジタルが１個のみか否かの判定と１個のみ存在する不正な部分ディジタル署名の決定手順について説明する。

【０１０９】

図９において、ｍ個の部分ディジタル署名

$$Sr(1)(M'), \cdots, Sr(m)(M')$$

の中に、正しい部分署名が少なくとも総合ディジタル署名作成のために必要な閾値ｋ個だけあり、かつ、図８に示す手順により、

$$Sr(1)(M'), \cdots, Sr(m)(M')$$

の中に不正なディジタル署名があると判定された場合に、その中の不正な部分ディジタル署名が１個のみか否かを判定し、１個のみ存在すると判定された場合に、その不正な部分ディジタル署名を決定する手続を示す。

【０１１０】

ステップ７１）　$S(M', I(i))^{e} \bmod N = H(M')$

が成り立たないようなｉ（$0 \leqq i \leqq m-1$）の集合をＦとおく。この判定は、上記の図８のステップ６３でも行ったものであり、図８の手順を実行するときに、同時にこのステップを実行してもよい。

【０１１１】

ステップ７２）　$0 \leqq i \leqq m-1$なる各ｉに対して、

$$F(i) = \{j \mid 0 \leqq j \leqq m-1 \text{かつ} r(i) \in I(j)\}$$

とおく。

【０１１２】

ステップ７３）　$0 \leqq i \leqq m-1$なるあるｊが存在して、Ｆ＝Ｆ（ｉ）が成り立つならば、不正な部分署名はSr(i)（M’）のみであると決定する。さもなければ、

$$Sr(1)(M), \cdots, Sr(m)(M)$$

の中には、不正な部分署名が２個以上あると判定する。

【０１１３】

Ｆ＝Ｆ（ｊ）となるような（$0 \leqq j \leqq m-1$）はあるとしても高々１つである

。m個の部分ディジタル署名

$$Sr(1)(M'), \cdots, Sr(m)(M')$$

の中に不正な部分ディジタル署名が複数あり、それらが結託して互いの不正の効果を打ち消しあうことにより、上記のステップ７４において、１≦ｉ≦ｍなるあるｉについて、Ｆ＝Ｆ（ｉ）となる可能性も想定できるが、３≦ｋ≦１０でｋ＋１≦ｒ≦２・ｋ－１という範囲ではこのようなことは起こらないことが計算機テストにより確認できる。

【０１１４】

上記の処理における処理量を評価する。

【０１１５】

ｋを統合ディジタル署名を作成するために必要な部分ディジタル署名ディジタル署名の数、即ち、閾値とし、ｒを部分ディジタル署名作成部の数とし、３≦ｋ≦１０とし、各ｋに対してｒ＝２・ｋ－１としたとき、鍵の長さが２０４８ビットの場合には、上記の手順で不正な部分ディジタル署名の存在の判定、及び不正な部分ディジタル署名が存在すると判定されたときに、不正な部分ディジタル署名が１つのみか否か、及び不正な部分ディジタル署名が１つのみと判定されたときに不正な部分ディジタル署名を決定するための処理量をｍｏｄＮでの乗算の数で評価すると、ｋ＝３のときは、部分署名に必要な処理量の０．１０倍、ｋ＝４のときは、部分署名に必要な処理量の０．１７倍、ｋ＝５のときは、部分署名に必要な処理量の０．２８倍、ｋ＝６のときは、部分署名に必要な処理量の０．４４倍、ｋ＝７のときは部分署名に必要な処理量の０．６９倍、ｋ＝８のときは部分署名に必要な処理量の０．９８倍，ｋ＝９のときは、部分署名に必要な処理量の１．４倍、ｋ＝１０の時は、部分署名に必要な処理量の２．０倍となる。

【０１１６】

従来、『T.Wu et al.「Building intrusion tolerant applications」, in Proceedings of 8th USENIX Security Symposium, USENIX, 1999』で提案されている検証法や、『S.Miyazaki et al.「On threshold RSA-signing with no dealer」in Proceedings of ICISC'99、LNCS Vol. 1787, pp. 197-207,Sprinter, 1999』で提案されている検証法では、部分ディジタル署名作成部が部分ディジタ

ル署名以外に、部分署名の正当性を検証するためのデータを追加して生成して、統合デジタル署名部に送信し、それを受信した統合ディジタル署名部が個々の部分ディジタル署名の正当性を検証するために、部分署名作成の2 倍以上の処理量を要している。従って、統合ディジタル署名作成に必要なｋ個の部分ディジタル署名の正当性検証に必要な処理量は、ｋ＝３のときは、部分署名に必要な処理量の６倍以上、ｋ＝４の時は、部分署名に必要な処理量の８倍以上、ｋ＝５のときは、部分署名に必要な処理量の１０倍以上、ｋ＝６のときは、部分署名に必要な処理量の１２倍以上、ｋ＝７のときは、部分署名に必要な処理量の１４倍以上、ｋ＝８のときは、部分署名に必要な処理量の１６倍以上、ｋ＝９のときは、部分署名に必要な処理量の１８倍以上、ｋ＝１０のときは、部分処理に必要な処理量の２０倍以上となる。

【０１１７】

上記の２つの処理量の評価を比較すると、本発明における不正な部分署名の検証方法は、上記の鍵長、閾値の数、及び部分ディジタル署名部の総数に対しては、必要な処理量が少ないという利点を持っていることがわかる。

【０１１８】

次に、全ての可能な統合ディジタル署名の作成法を用いる場合について説明する。

【０１１９】

また、部分ディジタル署名作成部の数が小さいときには、各々異なる部分ディジタル署名作成部により作成され、被署名ディジタル文書が一致するような部分署名の集合

$$Sr(1)(M'), \cdots, Sr(m)(M')$$

に対して、｛ｒ（１），…，ｒ（ｍ）｝の個数ｋ個の全ての部分集合

$$J(1), \cdots, J(K)$$

に対して、

【０１２０】

【数７】

$$S(M', J(i))^{e} \bmod N = H(M)$$

が成り立つか否かを試験し、Ｊ（ｉ）と当該試験結果との対応付けを検査することにより、不正な部分署名が２個以上あってもそれらを特定できる場合がある。ここでＫは、ｍ個からｋ個を選ぶ組み合わせの総数

$$m!/(k!\cdot(m-k)!)$$

である。例えば、統合ディジタル署名作成のための閾値が３で、部分ディジタル署名作成部の総数が５、かつ被署名ディジタル文書が一致する部分ディジタル署名が５個集まったときには、不正な部分署名が高々２個あっても、どの部分署名が不正かを決定することができることが、全ての場合を数え上げることにより確認できる。

【０１２１】

次に、図１０、図１１を用いて閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置について説明する。

【０１２２】

図１０は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置の構成図（その１）であり、図１１は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置の構成図（その２）である。

【０１２３】

図１０及び図１１において、分散ディジタル署名付ディジタル文書作成装置２は、複数の部分ディジタル署名作成部１３１，…，１３ｒ、統合ディジタル署名作成部１４、及び、ディジタル署名付ディジタル文書作成部１５とを有する。

【０１２４】

部分ディジタル署名作成部１３１，…，１３ｒは、入力されたディジタル文書Ｍに対して、各々独立に部分ディジタル署名

$$S1(M), \cdots, Sr(M)$$

を作成する。

【０１２５】

統合ディジタル署名作成部１４は、上記の複数の部分ディジタル署名作成部１３で独立に作成されたｍ個の部分ディジタル署名

$$Sr(1)(M), \cdots, Sr(m)(M)$$

（ｋ≦ｍ≦ｒかつｋ≦ｒ（１），…，ｒ（ｍ）≦ｒ）及び、当該ディジタル文書Ｍを受け取り、予め定めた閾値の個数ｋ個の部分ディジタル署名作成部の識別番号からなる１以上であるｓの集合

$$I1, \cdots, Is$$

に対して、出力された部分ディジタル署名から複数の統合ディジタル署名

$$S(M, I1), \cdots, S(M, Is)$$

を作成する。

【０１２６】

ディジタル署名付ディジタル文書作成部１５は、作成された統合ディジタル署名と入力されたディジタル文書を組み合わせ、当該ディジタル文書に対するディジタル署名付ディジタル文書を作成する。

【０１２７】

次に、上記の図１０、図１１の構成に付加情報結合部を設けた例を説明する。

図１２は、本発明の一実施例の閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置の構成図（その３）である。

【０１２８】

図１２において、分散ディジタル署名付ディジタル文書作成装置２は、複数の付加情報結合部１２１，…，１２ｒ と、複数の部分ディジタル署名作成部１３、統合ディジタル署名作成部１４及びディジタル署名付ディジタル文書作成部１５から構成される。

【０１２９】

付加情報結合部１２は、入力されたディジタル文書に各々独立に付加情報を付加し、付加情報付ディジタル文書１８を部分ディジタル署名作成部１３に出力する。

【０１３０】

部分ディジタル署名作成部１３１，…１３ｒは、入力された付加情報付ディジタル文書１８の部分ディジタル署名の組

（Ｍ‖α（ｉ，１），Ｓｉ（Ｍ‖α（ｉ，１）），…，

（Ｍ‖α（ｉ，ν（ｉ）），Ｓｉ（Ｍ‖α（ｉ，ν（ｉ））

（１≦ｉ≦ｒ）

を作成する。

【０１３１】

統合ディジタル署名作成部１４は、複数の部分ディジタル署名作成部１３で独立の作成された付加情報付ディジタル文書Ｍ’とその部分ディジタル署名のｍ個の組

（Ｍ’，Ｓｒ(1)（Ｍ’））…，（Ｍ’，Ｓｒ(ｍ)（Ｍ’））

（ｋ≦ｍ≦ｒかつ１≦ｒ（１），…，ｒ（ｍ）≦ｒ）を受け取り、予め定めた閾値の個数ｋ個の部分ディジタル署名作成部１３の識別番号からなる１以上のｓの集合

Ｉ１，…，Ｉｓ

に対して、出力された部分ディジタル署名から１以上であるｓ個の統合ディジタル署名

Ｓ（Ｍ’，Ｉ１），…，Ｓ（Ｍ’，Ｉｓ）

を作成する。

【０１３２】

ディジタル署名付文書作成部１５は、作成された付加情報付ディジタル文書とそれに対する統合ディジタル署名を組み合わせ、当該付加情報付ディジタル文書に対するディジタル署名付ディジタル文書Ｔを作成する。

【０１３３】

また、上記の実施例では、各構成図に基づいて説明したが、図３～図５に示す分散ディジタル署名作成装置の部分ディジタル作成部、統合ディジタル署名作成部及び、付加情報結合部についてプログラムとして構築することが可能であり、これらのプログラムを分散ディジタル署名作成装置として利用されるコンピュー

タのＣＰＵにインストールすることも可能である。

【０１３４】

また、構築されたプログラムをコンピュータに接続されるハードディスクや、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【０１３５】

また、図１１、図１２に示した分散ディジタル署名付ディジタル文書作成装置の作成装置の部分ディジタル作成部、統合ディジタル署名作成部及び、付加情報結合部及びディジタル署名付ディジタル文書作成部についてプログラムとして構築することが可能であり、これらのプログラムを分散ディジタル署名作成装置として利用されるコンピュータのＣＰＵにインストールすることも可能である。

【０１３６】

また、分散ディジタル署名作成装置と同様に、構築されたプログラムをコンピュータに接続されるハードディスクや、フロッピーディスク、ＣＤ－ＲＯＭ等の可搬記憶媒体に格納しておき、本発明を実施する際にインストールすることにより、容易に本発明を実現できる。

【０１３７】

なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【０１３８】

【発明の効果】

上述のように、本発明の閾値型分散ディタル署名作成装置によれば、信頼される第三者機関を含まないことによりディジタル署名のための秘密鍵を中心とする秘密鍵の漏洩をもたらす秘密漏洩の単一点を除くことにより、秘密鍵の安全性を中心とする署名システムの安全性を向上させ、同時に、複数ある部分ディジタル署名作成機関のうちの、予め定められた一定数が正常動作すれば、ディジタル署名の作成を可能とすることにより、ディジタル署名システムの耐攻撃性及び耐故障性を向上させ、これにより安全で、耐攻撃性及び耐故障性に優れた分散ディジタル署名作成システムが実現できる。

【図面の簡単な説明】

【図１】

本発明の原理を説明するための図である。

【図２】

本発明の原理構成図である。

【図３】

本発明の閾値個数の部分署名の組み合わせによる分散ディジタル署名作成装置の構成図（その１）である。

【図４】

本発明の閾値個数の部分署名の組み合わせによる分散ディジタル署名作成装置の構成図（その２）である。

【図５】

本発明の閾値個数の部分署名の組み合わせによる分散ディジタル署名作成装置の構成図（その３）である。

【図６】

本発明の第１の実施例の処理量が最小となるような部分ディジタル署名に対する変換指数の計算手順のフローチャートである。

【図７】

本発明の第１の実施例の部分ディジタル署名の組み合わせによる不正な部分ディジタル署名の検出法を説明するための図である。

【図８】

本発明の第１の実施例の部分ディジタル署名の組み合わせによる不正な部分ディジタル署名存在の判定手順のフローチャートである。

【図９】

本発明の第１の実施例の不正な部分ディタル署名が１個のみか否かを判定し、１個のみ存在する不正な部分ディジタル署名を決定する手順のフローチャートである。

【図１０】

本発明の第２の実施例の閾値個数の部分署名の組み合わせによる分散ディジタ

ル署名付ディジタル文書作成装置の構成図（その１）である。

【図１１】

本発明の第２の実施例の閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置の構成図（その２）である。

【図１２】

本発明の第２の実施例の閾値個数の部分署名の組み合わせによる分散ディジタル署名付ディジタル文書作成装置の構成図（その３）である。

【符号の説明】

１　分散ディジタル署名作成装置

２　分散ディジタル署名付ディジタル文書作成装置

１２　付加情報結合部

１３　部分ディジタル署名作成手段、部分ディジタル署名作成部

１４　統合ディジタル署名作成手段、統合ディジタル署名作成部

１５　ディジタル署名付ディジタル文書作成部

１６　部分ディジタル署名

１７　ディジタル文書と部分ディジタル署名の組

１８　付加情報付ディジタル文書

１９　付加情報付ディジタル文書と部分ディジタル署名の組

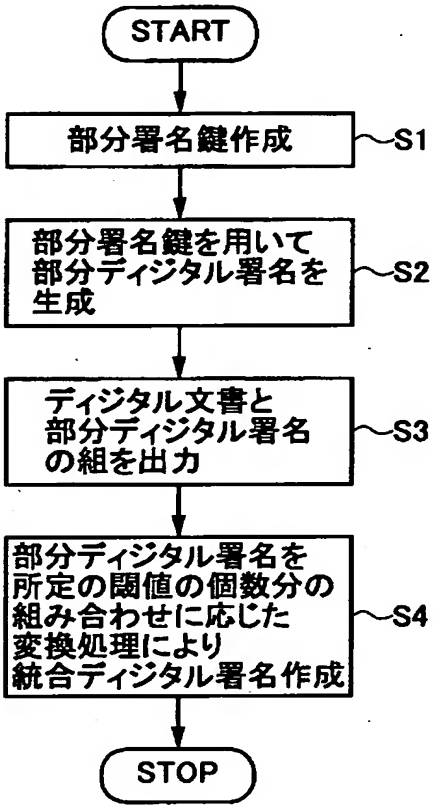
Ｍ　ディジタル文書

Ｔ　ディジタル署名付ディジタル文書

【書類名】　図面

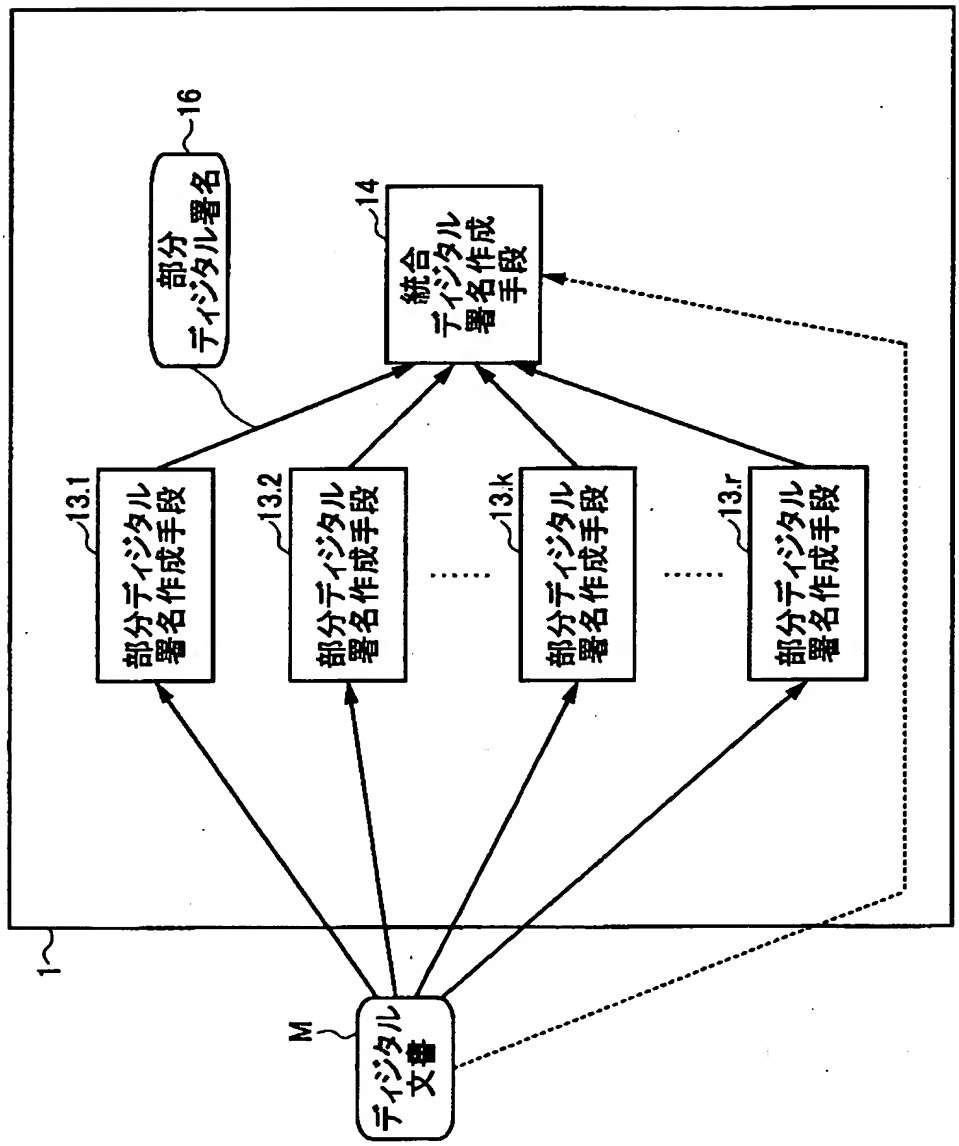
【図１】

本発明の原理を説明するための図



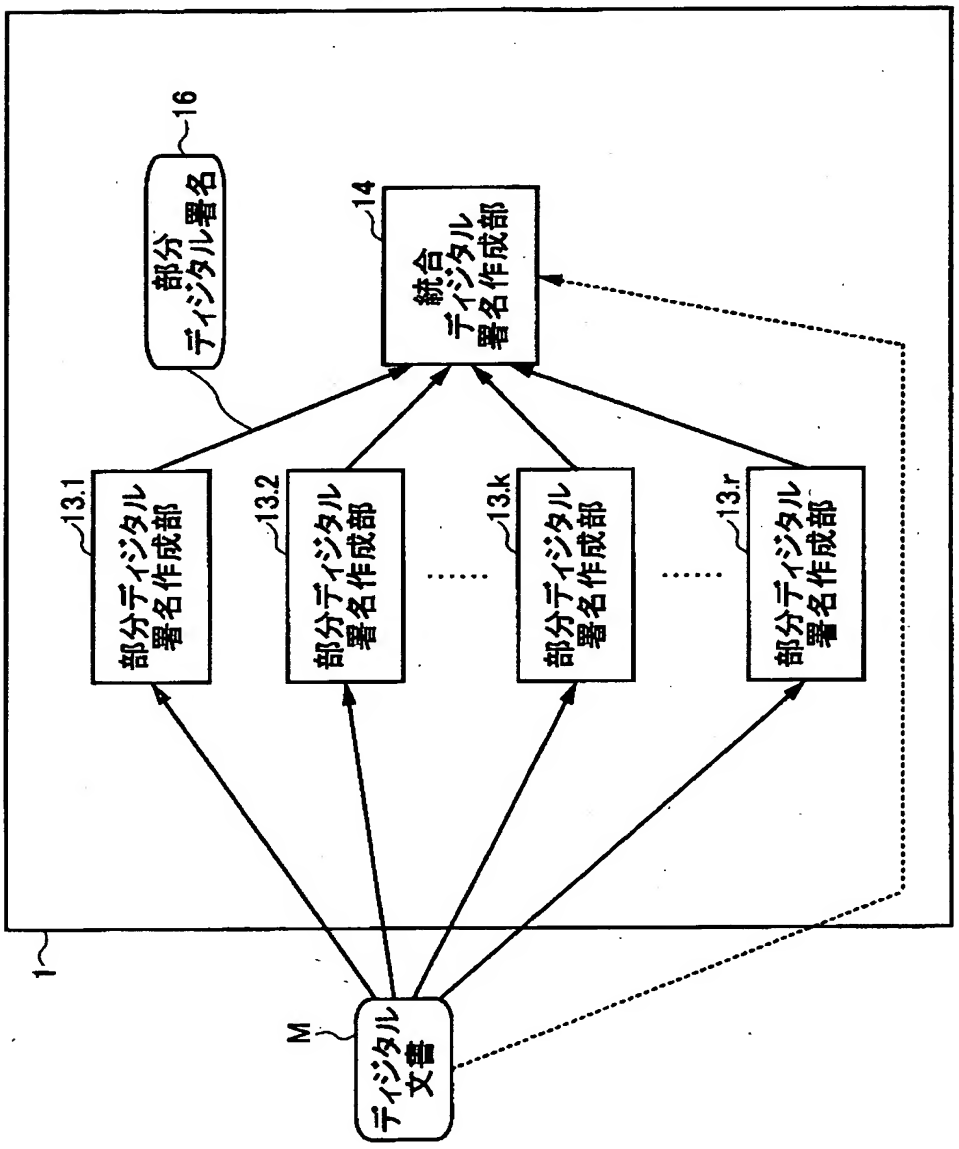
【図２】

本発明の原理構成図



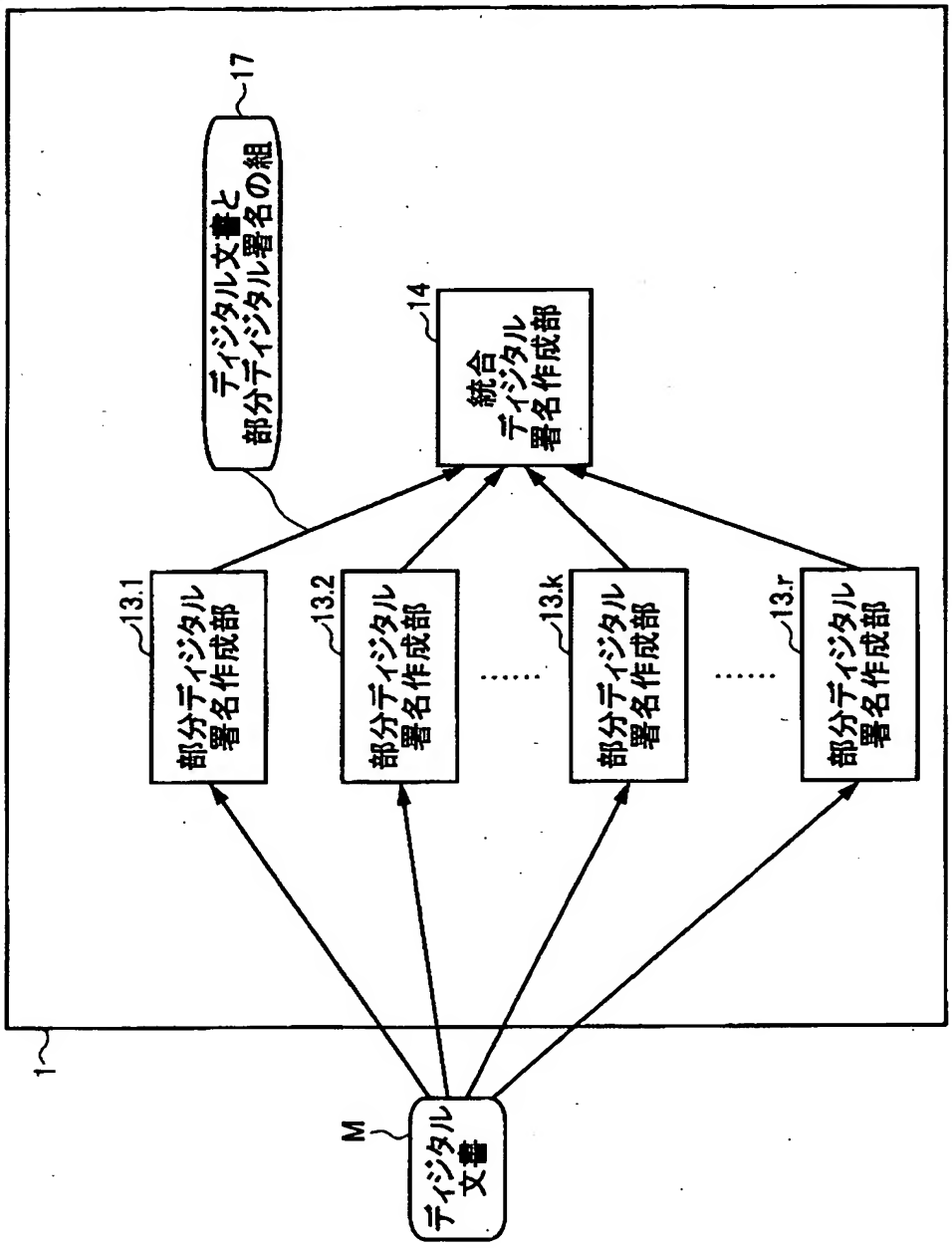
【図３】

本発明の閾値個数の部分署名の組合せによる
分散ディジタル署名作成装置の構成図（その１）



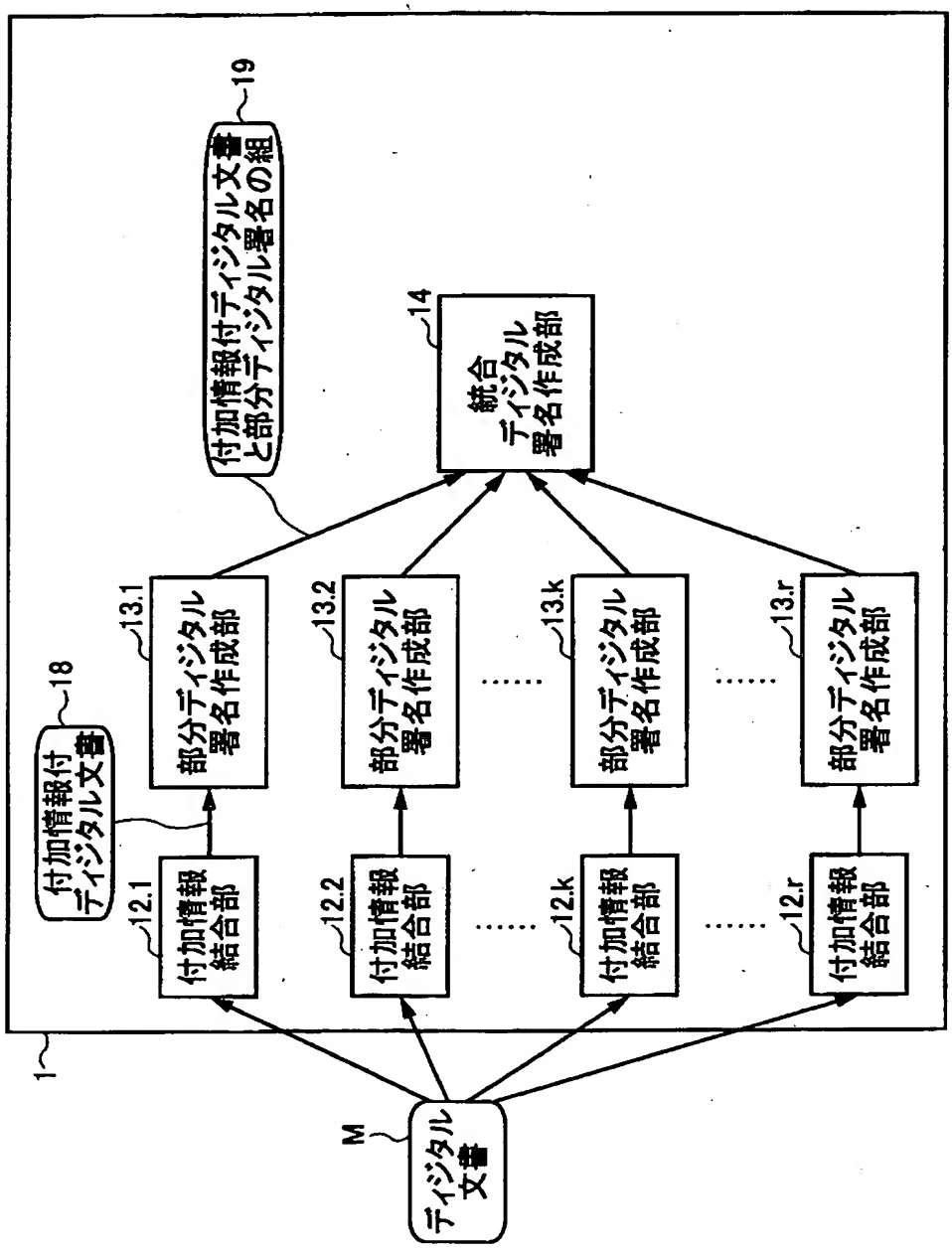
【図４】

本発明の閾値個数の部分署名の組合せによる
分散ディジタル署名作成装置の構成図（その2）



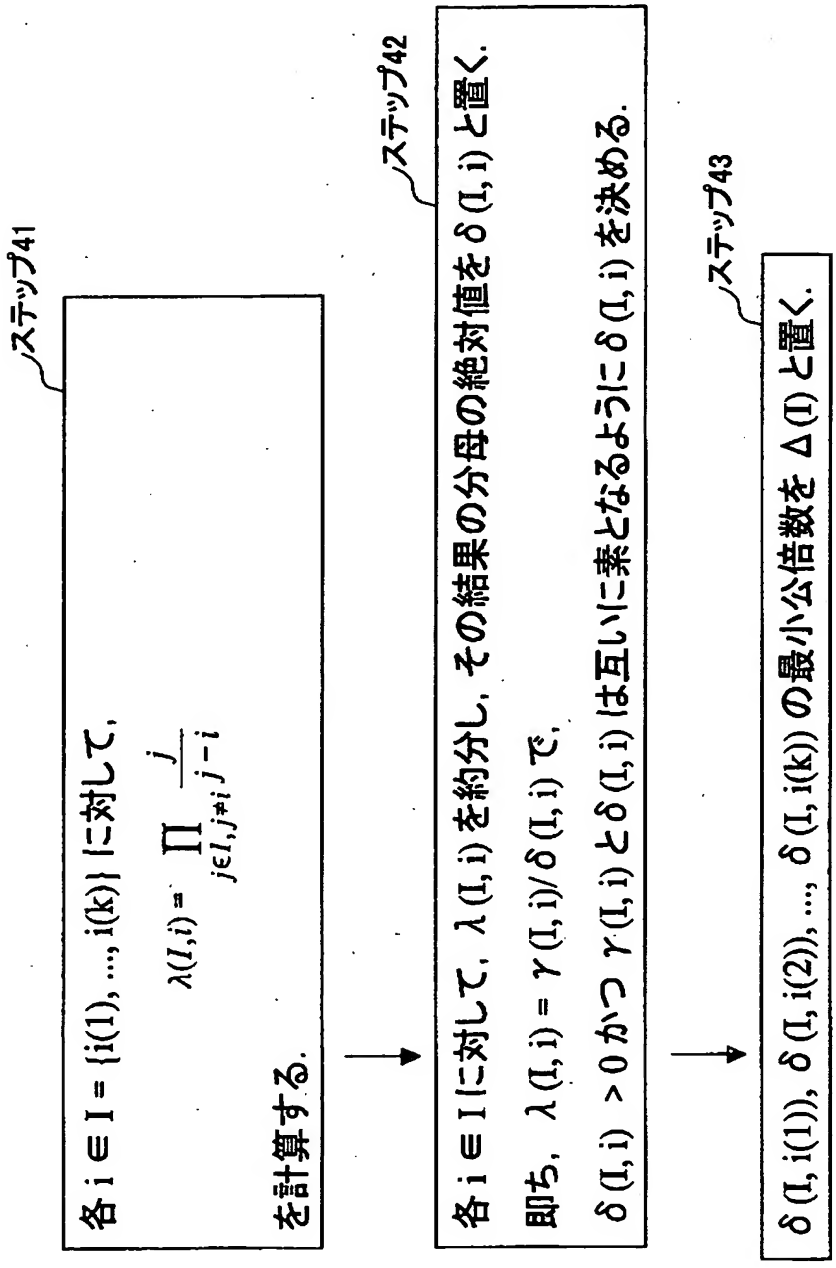
【図５】

本発明の閾値個数の部分署名の組合せによる
分散ディジタル署名作成装置の構成図（その３）



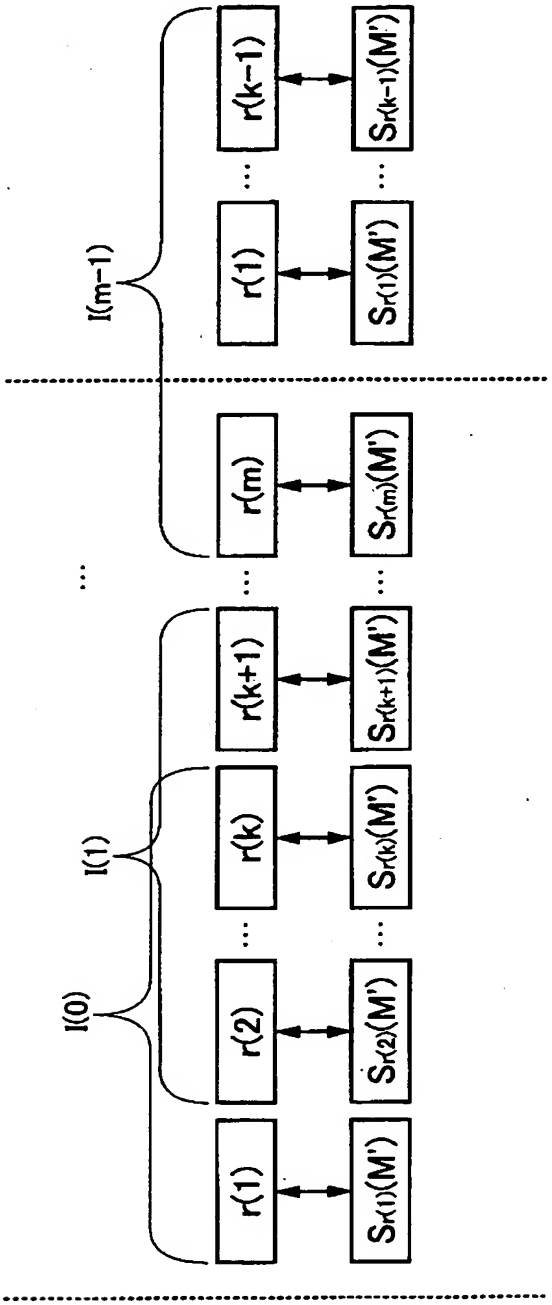
【図６】

本発明の第1の実施例の処理量が最小となるような
部分ディジタル署名に対する変換指数の計算手順のフローチャート



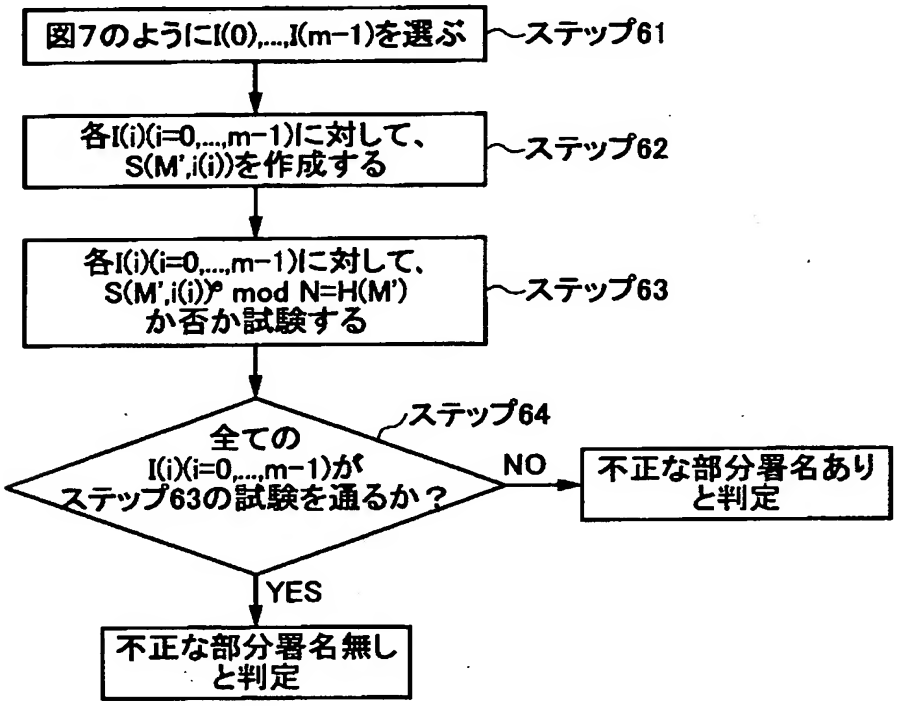
【図７】

本発明の第１の実施例の部分ディジタル署名の組合せによる不正な部分ディジタル署名の検出法を説明するための図



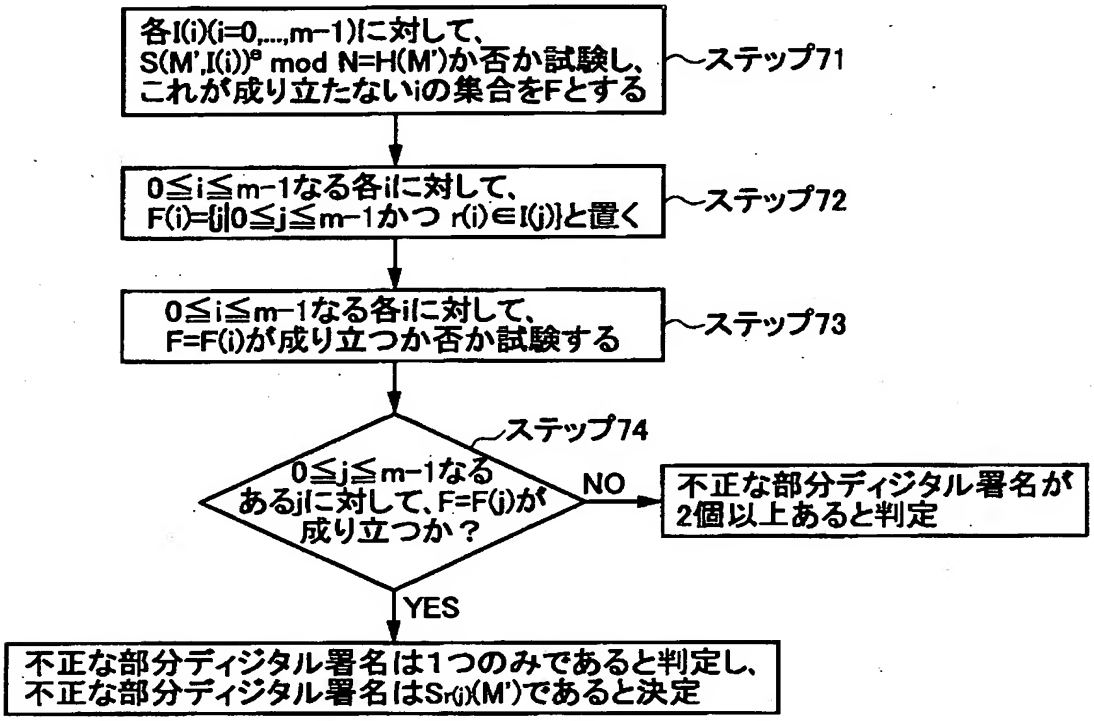
【図８】

本発明の第１の実施例の部分ディジタル署名の組合せによる不正な部分ディジタル署名存在の判定手順のフローチャート



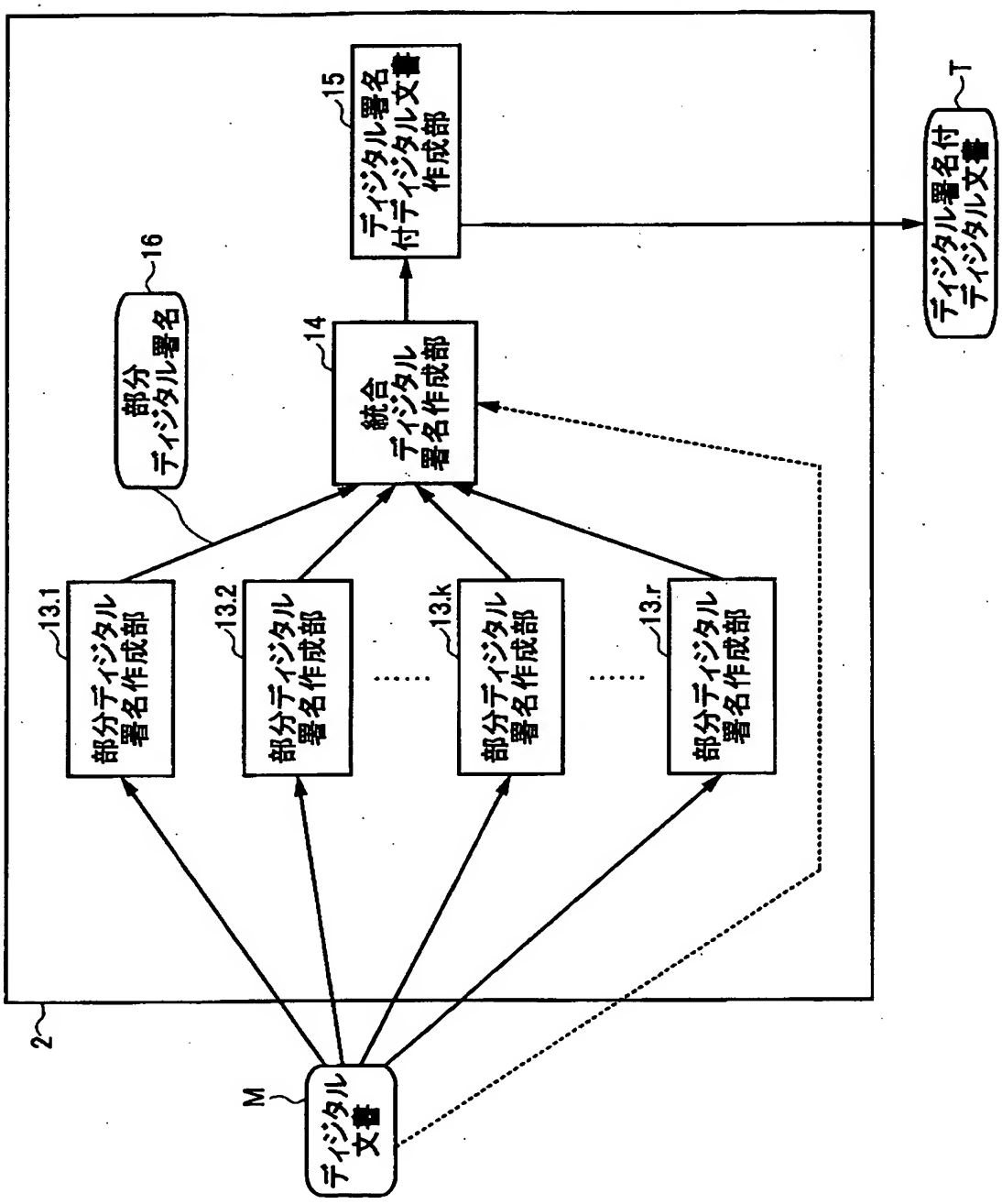
【図９】

本発明の第１実施例の不正な部分ディジタル署名が１個のみか否かを判定し一個のみ存在する不正な部分ディジタル署名を決定する手順のフローチャート



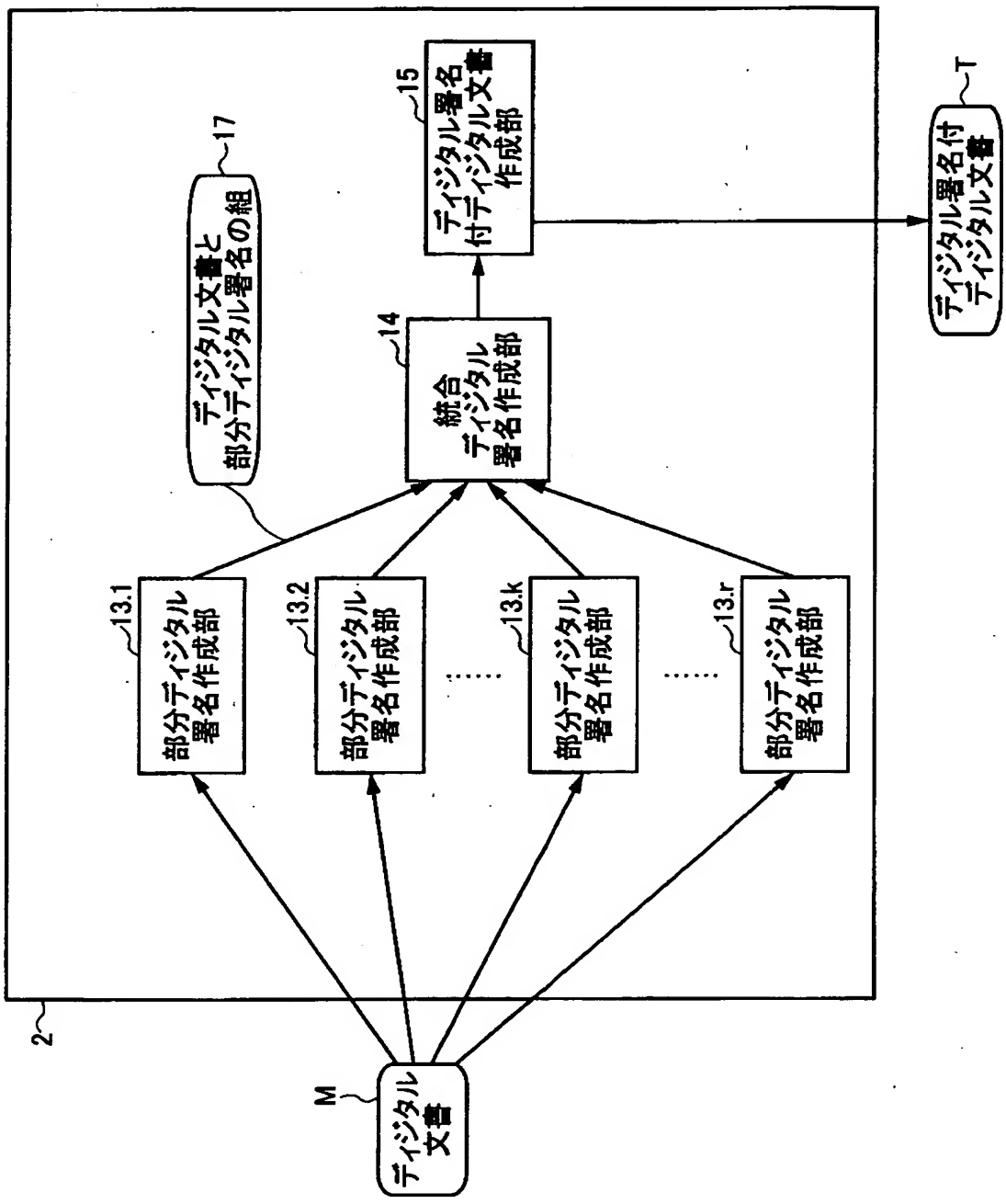
【図１０】

本発明の第2の実施例の閾値個数の部分署名の組合せによる分散ディジタル署名付ディジタル文書作成装置の構成図（その1）



【図１１】

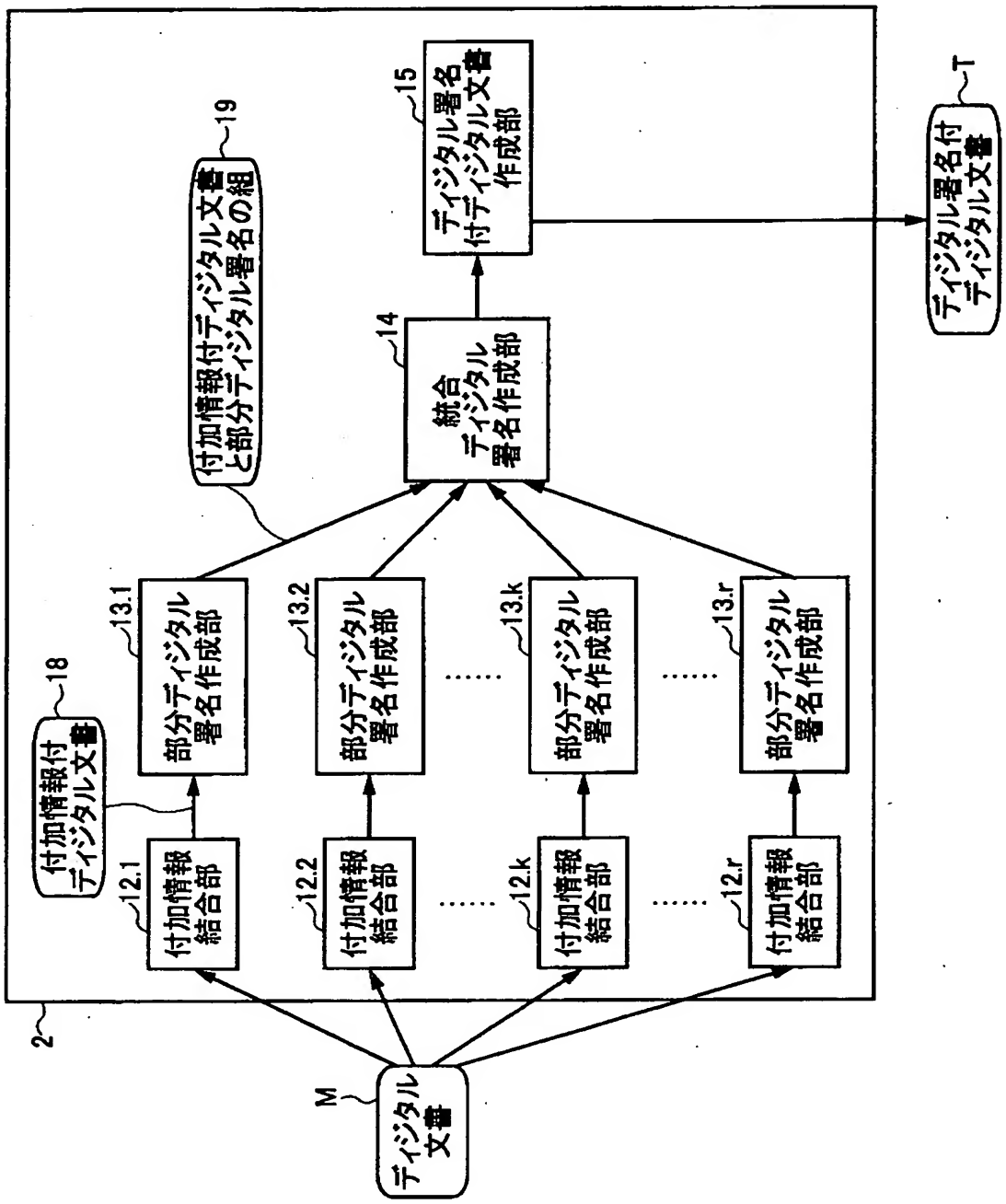
本発明の第2の実施例の閾値個数の部分署名の組合せによる分散ディジタル署名付ディジタル文書作成装置の構成図（その2）



出証特２００２－３０１６９５９

【図１２】

本発明の第2の実施例の閾値個数の部分署名の組合せによる分散ディジタル署名付ディジタル文書作成装置



【書類名】　　要約書

【要約】

【課題】　秘密漏洩の単一点を存在させず、かつ、部分ディジタル署名機関の全てのものが正しい部分ディジタル署名を作成しなければディジタル署名が作成できないようにする。

【解決手段】　本発明は、入力されるディジタル文書のハッシュ値に対して分散処理により生成された部分署名鍵を用いて各々の部分ディジタル署名を作成し、作成された部分ディジタル署名あるいは入力されたディジタル文書とその部分ディジタル署名の組を生成し、部分ディジタル署名を予め定められた閾値の個数だけ組み合わせて変換処理を行ない、統合ディジタル署名を作成する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４２２６〕

１．変更年月日　　１９９９年　７月１５日
［変更理由］　住所変更
住　所　　東京都千代田区大手町二丁目３番１号
氏　名　　日本電信電話株式会社